



Ralph Henne

**Die Kunst der Verschlüsselung
Einführung in die Kryptographie**

**Projekt für die 11. Jahrgangsstufe:
Objektorientierte Programmierung in Java**

Der Lehrplan Informatik der 11. Jahrgangsstufe fordert eine Projektarbeit im einem Rahmen von ca. 28 Std. Dieses Projekt soll von der Klasse selbstständig oder auch in konkurrierender Gruppenarbeit geplant und durchgeführt werden.

Ich habe mich für ein Projekt aus der Codierungstheorie entschieden. Auslöser war das Buch

Codes
Die Kunst der Verschlüsselung
Die Geschichte Die Geheimnisse Die Tricks
von Simon Singh

Innerhalb diese Projekt werden die Schüler vertraut mit folgenden Codierungsverfahren

1. Verschlüsselung nach Caesar
2. Verschlüsselung nach Trithemius
3. Verschlüsselung nach Viginere
4. Verschlüsselung mit Hilfe des RSA-Verfahrens

Das Team einer Projektarbeit besteht aus drei Gruppen mit jeweils ca. 4 Schülern. In der ersten Phase des Projekts arbeitet noch jeder Schüler für sich. Eine Vertiefung der gewonnenen Kenntnisse und Fertigkeiten erfolgt in der zweiten Phase. Die Schüler können hier bereits in Gruppenarbeit den Quellcode erstellen und sich gegenseitig helfen. In der dritten Phase der Projektarbeit müssen sich die drei Gruppen öfters zu einer Teambesprechung zusammensetzen, um das Projekt zu planen und zu koordinieren.

In der ersten Phase der Projektarbeit bearbeitet jeder Schüler einzeln das Kapitel 1 „Verschlüsselung nach Caesar“. Dieses Kapitel gibt einen ersten Einblick in die Codierungstheorie und in die Programmier Techniken in Java mit Hilfe von **BlueJ**. Es zeigt die Notwendigkeit, ein größeres Projekt in verschiedene Aufgaben aufzuteilen. Aus didaktischen Gründen besteht dieses erste Beispiel nur aus zwei Aufgaben, dem Codiervorgang und der grafischen Darstellung, die jeweils in einer separaten Klasse implementiert werden. **BlueJ** bietet die Möglichkeit, diese Klassen getrennt voneinander zu entwerfen und auch zu testen. Den Schülern wird nun bewusst, dass für das Zusammenwirken dieser Klassen in einer Gesamtanwendung eine Schnittstelle klar definiert werden muss. Mit „Schnittstelle“ meine ich die Teile einer Klasse, die anderen Klassen bekannt sind. Ich habe versucht, dieses Kapitel durch Beschreibung und Übungsaufgaben so zu gestalten, dass die Schüler selbstständig sich in ihr Projekt einarbeiten können.

In der zweiten Phase der Projektarbeit wird das Kapitel 2 „Verschlüsselung nach Trithemius“ innerhalb der Gruppe bearbeitet. Hier werden die

Programmierkenntnisse vertieft und die Gruppenarbeit geübt. Die Programmierung dieses Verschlüsselungsverfahrens stellt nur eine Erweiterung des Verfahrens nach Caesar dar. Hier kann also jeder in der Gruppe testen, ob er das Kapitel 1 verstanden worden hat. Nun stehen jeder Gruppe drei Klassen zur Verfügung, nämlich die beiden Codierungsverfahren „Caesar“ und „Trithemius“, sowie die grafische Oberfläche. Hier können sich die Gruppen zum ersten Mal über die Schnittstellen beraten, wie sich also diese drei Klassen zu einer Gesamtanwendung zusammensetzen lassen.

In der dritten Phase beginnt die eigentliche Projektarbeit und somit auch die Zusammenarbeit der drei Gruppen eines jeden Teams. Es sind folgende Aufgaben zu erledigen:

Gruppe 1: Verschlüsselung nach Viginere

Gruppe 2: Verschlüsselung nach dem RSA-Verfahren

Gruppe 3: Erstellen einer geeigneten grafischen Benutzungsoberfläche

Die ersten beiden Gruppen müssen sich in die Theorie der einzelnen Codierungsverfahren einarbeiten. Die Gruppe 3 erstellt die ersten Entwürfe der grafischen Benutzeroberfläche. Danach müssen in einer Teambesprechung die Schnittstellen zwischen den einzelnen Aufgabenteilen definiert werden. Hier helfen die Erfahrungen aus der zweiten Phase. In Gruppenarbeiten wird nun der jeweilige Quellcode implementiert, getestet und dokumentiert. Zum Schluss fügen die Gruppen ihre erarbeiteten Module zu einer Gesamtanwendung zusammen und erstellen eine Gesamtdokumentation.